



BRIT

writing the future
of cyber protection

XXXXXX
your CPR policy

Dear XXXXX

We are delighted you have purchased your Cyber Privacy Response (CPR) policy with Brit.

Please read the information contained in this welcome letter and all the documents attached, including:

- Product Pack
- Accuracy, Truth and Completeness of Application Information
- Declarations
- Policy Wording

The sums for which you are now insured are detailed in the Declarations. You also can see the total amount due.

Information provided by you

The cover we have provided to you is based upon the information you gave us in your application form. You can find this on the Accuracy, Truth and Completeness of Application Information document. Please read this information carefully to ensure that everything you have told us is accurate, true and complete. If, for any reason, this is no longer the case, then you must let us know as soon as possible as it may affect the validity of your CPR policy and our ability to pay a claim.

Datasafe

You now have complimentary access to Datasafe, which will allow you to proactively manage your exposures to data protection and privacy risk. Log on to Datasafe (<https://datasafe.britinsurance.com>) using your policy number, below:

XXXXXX

Questions

Should you have any questions about your CPR policy or concerns regarding the information you have provided to us or if you do not wish to continue with your CPR policy, please contact your broker.

Thank you for choosing Brit's CPR policy. We look forward to protecting your business.

Kind regards

Adelle Gruber

Class Underwriter

HAD A SECURITY BREACH? CALL OUR 24/7 CYBER RESPONSE HOTLINE:

(Please select the relevant number based on where you are calling from)

You also can download our Brit Cyber Response app for your phone.

Mainland Europe	+44 800 048 8965
UK	+44 800-048-8965
US/Canada	+1 (855) 440-3400
Latin America	+44 800 048 8965
South Africa	0800 995555
Australia	1800 465197
China	+44 800 048 8965
Hong Kong	+44 800 048 8965
Japan	+44 800 048 8965
Singapore	+44 800 048 8965



The background of the entire page is a photograph of several large satellite dishes. They are silhouetted against a twilight sky that transitions from a deep purple at the top to a lighter, hazy orange near the horizon. The sky is filled with numerous small, bright stars. The dishes are arranged in a receding line from the foreground towards the background, creating a sense of depth.

writing the future
of cyber protection

Cyber Privacy Response
your product pack

Datasafe

Datasafe delivers the latest risk management resources to proactively manage ever-evolving data protection and privacy risk, providing the ability to respond quickly and effectively in the event of a data breach

Training Resources

Keep employees up-to-speed on key privacy and data security issues:

- Assign online training courses to your employees and document course completion
- Industry-specific courses in HIPAA and PCI
- Ongoing awareness and training through bulletins, posters and webinars

Knowledge Center

Access over 500 online compliance and risk management resources including:

- Sample policies, procedures and agreements
- Cyber Fitness Check to assess your organization's cyber posture
- Incident Response Planning resources with sample plans and procedures
- State and industry-specific guidance on HIPAA, GLBA, and breach notification laws
- Guidance managing vendor risks with questionnaires and checklists

Virtual CISO

Leverage unlimited advice from privacy and data security experts to:

- Assist with typical tasks and duties of a Chief Information Security Officer
- Provide independent and unbiased advice to address data security concerns
- Supplement resources in the Knowledge Center

How to access Datasafe:

<https://datasafe.britinsurance.com>

In the event of an actual or suspected breach incident, it is imperative that you notify Brit as soon as possible through our 24/7 Cyber Response Hotline – which is a separate service from Datasafe. Not doing so can cause costly mistakes and increased liability. Please refer to the welcome letter in your policy pack for the Brit 24/7 Cyber Response Hotline.



Cover

Incident Response Services

Our panel of experts includes:

- Legal counsel specializing in privacy regulations who can quickly ascertain your legal obligations under the relevant jurisdictions
- IT forensic experts to help determine the cause and extent of your security breach
- Public relations firms to help manage potential negative press

The coverages provided for these services are subject to their own limit and do not reduce the limits elsewhere in the CPR policy. Full details can be found in your CPR policy and declarations.

Notification Services

Should your breach counsel determine that you need to notify individuals that their sensitive information has been compromised, the costs to do so will be covered by this section of your CPR policy.

Your breach counsel will help you notify:

- Regulators
- Affected Individuals

Notified individuals will be provided with a telephone hotline to access a call center where they will be able to enrol in credit monitoring and/or identity theft protection services. Full details can be found in your CPR policy and declarations.

The coverages provided for these services are subject to their own limit and do not reduce the limits elsewhere in the CPR policy

Insurance Protection

If, as a result of a privacy or security breach, you are investigated by a regulator, sued by a third party, suffer a business interruption loss or need to restore your digital assets, the CPR policy can respond to those claims and expenses.

Coverage options are available for:

- Business income and digital asset restoration
- Claims preparation costs
- Court attendance costs
- Cyber crime
- Cyber extortion threats and expenses
- Multimedia liability
- Payment card industry coverage (PCI-DSS)
- Privacy and security liability
- Regulatory investigations
- System hijacking
- And more

Full details about the cover you have can be found in your CPR policy and declarations.

Cyber experts are here to help you

24/7 cyber response hotline

Round the clock access to our toll-free hotline to report a cyber incident.

The breach coach

Dedicated legal counsel on hand as first responder to help organizations navigate their response and recovery to a cyber event including engaging with other vendors as required.

Breach response crisis management

Initial notification to the insured's clients (via mail / call center). Credit monitoring or identity protection services to mitigate any adverse impact.

Forensic investigation costs

Experts in IT who utilize specialized techniques to carefully examine and determine the cause and extent of the security breach.

Highly skilled forensic accountancy firms that will assist with economic damage calculations to help determine the extent of lost income as a result of a business interruption event.

Crisis Management and PR expenses

To manage the media and assist in repairing the company's reputation and restore trust in the event of a security breach

Your responsibilities

In the event of a breach

To benefit from your policy and associated services, you must follow the requirements stated in the policy and this CPR product pack.

To report an actual or suspected security or data privacy breach, you will need to call our 24/7 Cyber Response Hotline. You also can download our Brit Cyber Response app for your phone, which will connect you to the hotline.

For initial reporting, you should have available the following details:

1. Your company name and policy number; and
2. A brief description of the event and when it was first discovered.

We and our service providers require your prompt assistance and co-operation to provide the services under the policy. You must respond to all requests and enter into all necessary contracts with our vendors for the provision of their services in a timely manner.

To conduct their investigations, our IT experts will require access to your information, files and systems. Their findings will be made available to Brit and the CPR vendors involved in dealing with the incident.

IMPORTANT: Contacting the Brit Cyber Response Hotline does **not** satisfy the claim notification obligations under your CPR policy. Please also follow the **NOTICE** provisions of Section IX. Terms and Conditions in your CPR policy. All breaches or suspected breaches must be reported to: cpr.claims@britinsurance.com; your insurance broker; and any claim notification contact listed on your CPR policy's declarations as "Notice of Claim, Circumstance or Loss" in accordance with the **NOTICE** provisions of your CPR policy.



Cyber Privacy Response

IMPORTANT INFORMATION

Truth, Accuracy and Completeness of Application Information

Please read the responses you have provided to us in your application form summarized below and check these are true, accurate and complete.

Should any of the information not be true, accurate and complete you must let us know as soon as possible and no later than the inception date of your CPR policy. Once your CPR policy has inceptioned and you are covered by your CPR policy, you must also let us know if the information you have provided is or may no longer become true, accurate or complete. On receipt of your updated information, we will advise you whether this affects the terms and conditions of your CPR policy. Further, we draw your attention to your obligations contained in Section IX. Terms and Conditions of your CPR policy.

Where the information provided by you is and remains true, accurate and complete, we do not need any further information.

Please note that if you do not tell us of any changes to the information you have provided it may affect the validity of your CPR policy and our ability to pay a claim.

Annual Revenue	Number of Records	Main Business Description

You and Your Business

We asked you	You answered
What is your main Business Description?	
1. Does the applicant use Google Workspace, Microsoft 365 or other similar cloud-based infrastructure with the four network security best practices listed in Question 2 implemented and maintained? (if yes, continue to Question 3)	
2. Which of the following security best practices does the applicant implement and maintain on its network(s): <ul style="list-style-type: none">Filtering all incoming emails and communications for malicious links, spam, malware and attachments?Multi-Factor Authentication for all accounts of all kinds on the network(s)?Sender Policy Framework?Endpoint monitoring and anti-virus capability (if no, answer below)<ul style="list-style-type: none">Does the applicant use cloud security monitoring tooling/dashboards to ensure a secure configuration is being used? (if no, answer below)Please provide full details of compensatory controls.	
3. Does the applicant implement and maintain the following protocols <ul style="list-style-type: none">All system configuration and data is either (i) subject to regular back-ups (at least weekly) via secure cloud or (ii) maintained in offline copies disconnected from the organisation's network?Multi-factor authentication settings are enabled for access to back-up files?Data is encrypted while it is in transitData is encrypted while at rest, including while on portable devices	
4. Does the applicant implement within 14 days all critical security, anti-virus and malware patches/signatures received from commercial software vendors onto all of its servers, laptops, desktops, routers, firewalls, phones and other physical devices? (if no, answer below)	
Within how many days are critical security, anti-virus and malware patches received from commercial software vendors implemented on all physical devices? No. of days:	

<p>5. Does the applicant confirm that</p> <ul style="list-style-type: none"> • none of its directors or officers are aware of any claims or circumstances that may give rise to a claim or loss under this proposed insurance, or would have given rise to a claim or loss under this proposed insurance had it been in force at the time, including any computer system intrusion, tampering, virus or malicious attack, loss of data, hacking incident, alleged data theft, unplanned outage or similar circumstances, which has exceeded USD 5,000 in total costs? <p>Provide answer:</p>	
<ul style="list-style-type: none"> • It provides all employees with anti-fraud training at least annually (including but not limited to detecting social engineering, phishing simulation and security & privacy awareness training, business email compromise and other similar exposures); and before processing funds transfers and/or third-party account detail changes, confirm the transaction details with the requestor, through a secondary means of communication***? <p>***A “secondary means of communication” is different from the first means of communication. For example, if the request is received by telephone, a secondary communication may be an email.</p>	
<p>6. Is the applicant</p> <ul style="list-style-type: none"> • a platform / app provider (or developer) for any of the following: money / funds / securities transfer, cryptocurrencies / blockchain, crowd-funding, fundraising, political lobbying, direct / targeted marketing, social media, dating, gaming, file sharing or content streaming? • involved in: adult entertainment, debt collection the processing, storage or distribution of cannabis products, emergency services, technology development application/service/platform hosting, or customer software development? 	

Company and Subsidiary Turnover Breakdown		
Company Name	Country	Share of Overall Turnover

Declarations

POLICY NUMBER: XXXXX

UMR: XXXXX

NAME INSURED: XXXXX

ADDRESS: XXXXX

POLICY PERIOD: FROM XXXXX TO XXXXX (both days at 12:01 AM (midnight) local time at the address shown above)

Policy Aggregate Limit of Liability:	USD XXXXX	
Limits and Sublimits by Coverage:		
A. Privacy and Security Liability and Regulatory Claims	USD XXXXX	
B. Breach Response Services		Coverage for Breach Response Services is separate from and in addition to the Policy Aggregate Limit of Liability but subject to these aggregate limits for all Privacy Breaches and Security Breaches . Upon exhaustion of these limits, any additional costs for Breach Response Services may erode the Policy Aggregate Limit of Liability at discretion of the Named Insured .
Incident Response Services	USD XXXXX	
Notification Services	XXXXX Affected Individuals	
C. PCI DSS Assessments	USD XXXXX	
PCI Recertification Expenses	USD XXXXX	
D. Cyber Extortion	USD XXXXX	
E. Business Income Loss	USD XXXXX	
F. Digital Asset Restoration	USD XXXXX	
G. Multimedia Liability	USD XXXXX	
H. Cyber Crime	USD XXXXX	Aggregate sublimit for all Crime Loss
I. Invoice Manipulation	USD XXXXX	Aggregate sublimit for all Invoice Manipulation Loss
J. System Hijacking	USD XXXXX	Aggregate sublimit for all System Hijacking Loss
K. Supplemental Coverages Post Breach Remedial Consulting Reputational Harm Claims Preparation Costs Court Attendance Costs Criminal Reward Payments	XXXXX Hours USD XXXXX USD XXXXX USD XXXXX USD XXXXX	Aggregate sublimit for each Supplemental Coverage is shown
Retentions:		
Breach Response Services	USD XXXXX	Each Privacy Breach or Security Breach
Retention for Affected Individuals	XXXXX	Each Privacy Breach or Security Breach
All Other Coverages(s):	USD XXXXX	
Waiting Period	XXXXX Hours	
Total Premium (includes broker commission) * (Excluding additional Taxes and Surcharges as applicable)	USD XXXXX	

CONTINUITY DATE: XXXXX

CHOICE OF LAW: State of New York

NOTICE OF CLAIM, CIRCUMSTANCE OR LOSS: cpr.claims@britinsurance.com

SERVICE OF SUIT: Lloyd's America, Inc. Attention: Legal Department 280 Park Avenue, East Tower, 25th Floor New York, NY 10017

SCHEDULE OF FORMS AND ENDORSEMENTS

<u>Endorsement / Form No.:</u>	<u>Title</u>
LMA 3100	Sanctions Limitation and Exclusion Clause
LMA 5389	U.S. TERRORISM RISK INSURANCE ACT OF 2002 AS AMENDED - NEW & RENEWAL BUSINESS ENDORSEMENT
BRT10150819	Lloyd's Security Schedule and Several Liability Notice
LSW 1135B	Lloyd's Privacy Policy Statement
LSW 3000	Premium Payment Clause (60 Days)
Biometric	Biometric information exclusion
CPRPS2021V1e001	Professional Service exclusions endorsement - generic (no E&O overlap)
LMA 9038	FLORIDA SURPLUS LINES NOTICE (RATES AND FORMS)
Manuscript	No coverage under section G Multimedia

SANCTIONS LIMITATION AND EXCLUSION CLAUSE

No (re)insurer shall be deemed to provide cover and no (re)insurer shall be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America.

LMA3100

9/2010

**Terrorism Risk Insurance Act of 2002 as amended
New & Renewal Business Endorsement**

This Endorsement is issued in accordance with the terms and conditions of the "Terrorism Risk Insurance Act of 2002" as amended, as summarized in the disclosure notice.

In consideration of an additional premium of USD 0 paid, it is hereby noted and agreed with effect from inception that the Terrorism exclusion to which this Insurance is subject, shall not apply to any "insured loss" directly resulting from any "act of terrorism" as defined in the "U.S. Terrorism Risk Insurance Act of 2002", as amended ("TRIA").

The coverage afforded by this Endorsement is only in respect of any "insured loss" of the type insured by this Insurance directly resulting from an "act of terrorism" as defined in TRIA. The coverage provided by this Endorsement shall expire at 12:00 midnight December 31, 2027, the date on which the TRIA Program is scheduled to terminate, or the expiry date of the policy whichever occurs first, and shall not cover any losses or events which arise after the earlier of these dates. The Terrorism exclusion, to which this Insurance is subject, applies in full force and effect to any other losses and any act or events that are not included in said definition of "act of terrorism".

This Endorsement only affects the Terrorism exclusion to which this Insurance is subject. All other terms, conditions, insured coverage and exclusions of this Insurance including applicable limits and deductibles remain unchanged and apply in full force and effect to the coverage provided by this Insurance.

Furthermore the Underwriter(s) will not be liable for any amounts for which they are not responsible under the terms of TRIA (including subsequent action of Congress pursuant to the Act) due to the application of any clause which results in a cap on the Underwriter's liability for payment for terrorism losses.

LMA5389

09 January 2020

NAMED ASSURED: XXXXX

Policy Reference: XXXXX

Effective Date of Endorsement: XXXXX

Endorsement No. XX

LLOYD'S SECURITY SCHEDULE AND SEVERAL LIABILITY NOTICE

Syndicate 2987 100%

The subscribing insurers' obligations under contracts of insurance to which they subscribe are several and not joint and are limited solely to the extent of their individual subscriptions. The subscribing insurers are not responsible for the subscription of any co-subscribing insurer who for any reason does not satisfy all or part of its obligations.

LLOYD'S PRIVACY POLICY STATEMENT

UNDERWRITERS AT LLOYD'S, LONDON

The Certain Underwriters at Lloyd's, want you to know how we protect the confidentiality of your non-public personal information. We want you to know how and why we use and disclose the information that we have about you. The following describes our policies and practices for securing the privacy of our current and former customers.

INFORMATION WE COLLECT

The non-public personal information that we collect about you includes, but is not limited to:

- Information contained in applications or other forms that you submit to us, such as name, address, and social security number
- Information about your transactions with our affiliates or other third-parties, such as balances and payment history
- Information we receive from a consumer-reporting agency, such as credit-worthiness or credit history

INFORMATION WE DISCLOSE

We disclose the information that we have when it is necessary to provide our products and services. We may also disclose information when the law requires or permits us to do so.

CONFIDENTIALITY AND SECURITY

Only our employees and others who need the information to service your account have access to your personal information. We have measures in place to secure our paper files and computer systems.

RIGHT TO ACCESS OR CORRECT YOUR PERSONAL INFORMATION

You have a right to request access to or correction of your personal information that is in our possession.

CONTACTING US

If you have any questions about this privacy notice or would like to learn more about how we protect your privacy, please contact the agent or broker who handled this insurance. We can provide a more detailed statement of our privacy practices upon request.

06/03

LSW1135B

PREMIUM PAYMENT CLAUSE

The (Re)Insured undertakes that premium will be paid in full to Underwriters within 60 days of inception of this policy (or, in respect of instalment premiums, when due).

If the premium due under this policy has not been so paid to Underwriters by the 60th day from the inception of this policy (and, in respect of instalment premiums, by the date they are due) Underwriters shall have the right to cancel this policy by notifying the (Re)Insured via the broker in writing. In the event of cancellation, premium is due to Underwriters on a pro rata basis for the period that Underwriters are on risk but the full policy premium shall be payable to Underwriters in the event of a loss or occurrence prior to the date of termination which gives rise to a valid claim under this policy.

It is agreed that Underwriters shall give not less than 15 days prior notice of cancellation to the (Re)Insured via the broker. If premium due is paid in full to Underwriters before the notice period expires, notice of cancellation shall automatically be revoked. If not, the policy shall automatically terminate at the end of the notice period.

Unless otherwise agreed, the Leading Underwriter (and Agreement Parties if appropriate) are authorised to exercise rights under this clause on their own behalf and on behalf of all Underwriters participating in this contract.

If any provision of this clause is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability will not affect the other provisions of this clause which will remain in full force and effect.

Where the premium is to be paid through a London Market Bureau, payment to Underwriters will be deemed to occur on the day of delivery of a premium advice note to the Bureau.

LSW3000

ENDORSEMENT attaching to and forming part of Policy No. XXXXX

NAMED ASSURED: XXXXX

Effective date of this endorsement: XXXXX

EXCLUSION RE BIOMETRIC INFORMATION

It is understood and agreed that the following exclusion is added to Section **IV. EXCLUSIONS**:

Any **Claim** based upon, arising out of or resulting from the unlawful collection, use, processing, retention, storage or disposal of biometric information, data or identifiers by **You** or on **Your** behalf.

NAMED ASSURED: XXXXX
EFFECTIVE DATE: XXXXX
POLICY REFERENCE: XXXXX
POLICY PERIOD: From XXXXX to XXXXX

EXCLUDE PROFESSIONAL SERVICES CLAIMS

It is understood and agreed that the following exclusion is added to Section **IV. EXCLUSIONS**:

Any **Claim** arising out of an act, error or omission by **You** in the rendering of or failing to render professional services for others;
All other terms and conditions remain unchanged.



FLORIDA SURPLUS LINES NOTICE (RATES AND FORMS)

**SURPLUS LINES INSURERS' POLICY RATES AND FORMS ARE NOT APPROVED
BY ANY FLORIDA REGULATORY AGENCY.**

Insured Name XXXXX
Insurer XXXXX
BRT6FL20220

Policy No. XXXXX
Effective Date XXXXX
Page 1 of 1




Brit Syndicates Limited

The Leadenhall Building
122 Leadenhall Street
London
EC3V 4AB

T: +44 (0)20 3857 0000

GCPT@britinsurance.com

www.britinsurance.com

A photograph of several white wind turbines on a grassy hill. The turbines are set against a clear blue sky with a few wispy clouds. In the background, there is a body of water and distant hills. The overall scene is bright and sunny.

Brit Syndicates Limited is authorized and regulated by the Prudential
Regulation Authority and regulated by the Financial Conduct Authority